POLICY

Effective Date: May 1, 2009
Approved By: WWU Board of Trustees

See Also: POL-U5300.01 Safeguarding Non-Public Financial Information
Fair and Accurate Credit Transactions Act of 2003 (FACTA)
Gramm-Leach-Bliley Act (GLBA)

POL-U3000.01 IDENTIFYING, DETECTING AND RESPONDING TO IDENTITY THEFT RED FLAGS AND NOTICES OF ADDRESS DISCREPANCIES

This policy applies to all university employees who are responsible for, have access to, or handle covered accounts as described below.

Definitions:

Federal Trade Commission (FTC) Red Flag Rule: The rule requires "financial institutions" **and** "creditors" that hold "covered accounts" to develop and implement an identity theft prevention program for new and existing accounts.

Red Flag: Red Flags are patterns, practices, and specific activities that signal possible attempted fraud via identity theft on covered accounts.

Covered Account: Covered account for the purpose of this policy includes, any type of account or payment plan that involves multiple transactions or multiple payments in arrears. Covered accounts include loans through the Federal Perkins Loan program, the Federal Family Education Loan Program, institutional loans, and fees collected in arrears.

Creditor: Any entity that defers payment for services rendered; that regularly arranges for the extension, renewal or continuation of credit; or any assignee of an original creditor who is involved in the decision to extend, renew, or continue credit.

Identifying Information: Any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including name, social security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, unique physical representation, unique electronic identification number or address, or telecommunication identifying information.

Identity Theft: A fraud committed or attempted using the identifying information of another person without authority.

Service Providers: Service providers refer to all third parties who, in the ordinary course of university business, are provided access to covered accounts. Service providers may include,

but are not limited to, collection agencies, loan processing agencies, and systems support providers.

1. University Maintains an Identity Theft Prevention Program

A. The purpose of the university's Identity Theft Prevention Program is to detect, prevent and mitigate fraud attempts via identity theft in connection with the opening of a covered account or any existing covered account by:

i. Identifying relevant financial processing red flags for covered accounts signaling possible fraud attempt via identity theft and incorporating those red flags into the program;
ii. Establishing procedures to detect red flags that have been incorporated into the program; and
iii. Responding appropriately to any red flags that are detected to prevent and mitigate identity theft related to financial transactions.

B. The WWU Technology Security Incident Response Program provides mechanisms to:

i. Bring critical strategic personnel on campus together.
ii. Determine the extent of the risk and violation.
iii. Designate the proper action.

C. The Financial Information Security Program provides mechanisms to:

i. Identify and assess the risk factors related to covered accounts;
ii. Develop written procedures to manage and control these risks and carry out the activities described in (A) above;
iii. Train appropriate staff in the program activities; and
iv. Adjust the plan to reflect the University's experiences with identity theft, changes in methods of identity theft or methods to detect, prevent and mitigate identity theft, and changes related to the offering or managing of covered accounts.

This program will be a component of the overall campus-wide Information Technology (IT) Security Plan. The IT Security Plan will be administered by the WWU Chief Information Officer. The IT Security Plan will prevail if a conflict arises.

2. Chief Information Officer (CIO), in Consultation with the Vice President for Business and Financial Affairs, Appoints the University's Identity Theft Prevention Program Coordinator and Authorizes Program Activities

A. The CIO, in consultation with the Vice President for Business and Financial Affairs, appoints the university's Identity Theft Prevention Program Coordinator and authorizes

the activities necessary for the Coordinator to implement and maintain the program. This Red Flag program will be reviewed for compliance with the IT Security Plan by the CIO.

3. CIO Appoints the University's Identity Theft Prevention Program Oversight Committee

The CIO will appoint managers from relevant university departments to serve on the Oversight Committee. These departments may include, but are not limited to, Student Financial Services, Financial Aid, Administrative Computing Services, Internal Audit, and Business and Financial Affairs Internal Control Officer.

4. Incident Response

All possible identity theft instances will be reported to the CIO. The CIO will call the Security Incident Response Team together for review and designated action per the IT Security Plan.

5. Identity Theft Prevention Coordinator Submits Report on Program Compliance at Least Annually

At least annually, or more frequently if an elevated level of risk so warrants, the Identity Theft Prevention Coordinator will present a written report of material program matters to the Board of Trustees Audit Committee, Vice President for Business and Financial Affairs, the CIO, the Security Incident Response Team, and the Oversight Committee. The report will include:

a. The activities of the program;
b. The effectiveness of the program in addressing the risk of identity theft;
c. Service provider arrangements; and
d. Significant incidents involving identity theft and management's response.

6. Contract Administrator Ensures Covered Account Service Providers Bid Documents and Contracts Comply with FTC Red Flag Rule

The Contract Administrator ensures that any covered account service provider bid documents and any subsequent contract negotiated includes the requirement for compliance with the FTC's Red Flag Rules.

7. University Periodically Reviews and Adjusts the Identity Theft Prevention Program

The Coordinator, in conjunction with the Oversight Committee, will periodically review and adjust the Identity Theft Prevention Program to reflect changes in risks to customers or to the safety and soundness of the university from identity theft.